February 20, 2019

Honorable Mark Warner
United States Senate
703 Hart Senate Office Building
Washington, DC 20510

Dear Senator Warner:

Thank you for your January 30, 2019, letter requesting information about the Facebook Research Application (the "App"). Initial reporting around this project was not entirely accurate, so we appreciate the opportunity to share some additional information about the App and to answer your questions based on our review to date.

Like many companies, we invite people to participate in research that helps us identify things we can be doing better. The App was part of this market research. We worked with third-party research vendors to invite participants to download software on their devices that allows us to better understand how people use their mobile devices. At the time we ended the Facebook Research App on Apple's iOS platform, less than 5 percent of the people sharing data with us through this program were teens. Analysis shows that number is about 18 percent when you look at the complete lifetime of the program, and also add people who had become inactive and uninstalled the app.

Each user was required to complete a clear consent flow prior to participation. Potential participants were required to confirm that they were over 18 or provide other evidence of parental consent, though the vendors did not require a signed parental consent form for teen users. We don't share the information we collect through the App with others, and people can stop participating at any time.

Despite early reports to the contrary, the participants in this research project were notified, through clear consent flows and disclosures during the registration and installation process, that this was a Facebook app that would collect their data. In summary, potential participants were required to register with the vendor, agree to participate in the research, and access a website on the facebook.com domain, bearing the heading "Facebook Study," to download and install an app called "Facebook Research" and certificates that allowed this app to function. Throughout this process, potential participants were repeatedly informed and required to acknowledge that this was a Facebook app, that their data would be collected by Facebook, and that they could withdraw from the project and uninstall the App at any time. To participate, potential participants were also repeatedly required to consent to participation in the survey, to consent to downloading and installing the App, and consent to granting Facebook permission to access internet browsing and app usage activity and data. While the language used in the flows varied over time,

Address: 1601 Willow Road
Menlo Park, CA 94025

the following paragraphs walk through an example of this process, providing sample screenshots of the iOS experiences as examples of the disclosures, and consents a user saw.

Registration
First, potential participants were required to register with one of the vendors, who are experienced and well-reputed market research companies who recruit participants for many other companies' market research programs, and agree to participate in the research. Participants provided their contact information and date of birth. The vendors provided clear guidance in the online registration process requiring potential participants to confirm that they were over 18, or prompted them to provide other evidence of parental consent. Specifically, if under 18, participants were required to provide the email address associated with their parent's PayPal account in order to receive payment; PayPal requires users to be 18 or the age of majority in their respective jurisdictions. During the registration process, participants were informed that they would be downloading software that would allow access to their internet browsing and app usage activity and data. The following disclosures were those used by two vendors during the onboarding flow.

First:

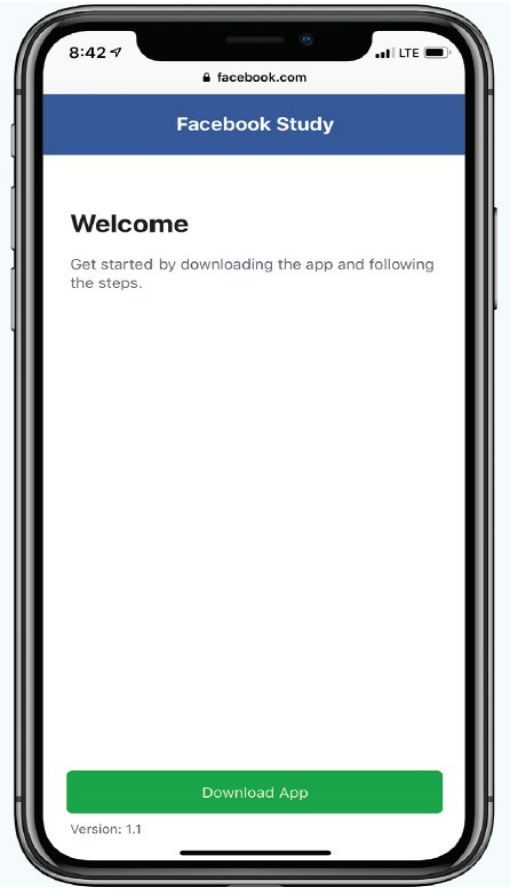
> *Thank you for participating in our research about how people use apps. This research helps our client understand how people use mobile apps so we can improve our services and introduce new features for millions of people around the World. In order to do this, we ask that you install our client's research software on your phone. Here, we'll explain a bit how information is collected from this software and what it means for you. By installing the software, you're giving our client permission to collect data from your phone that will help them understand how you browse the internet, and how you use the features in the apps you've installed. This data will only be used by our client, and won't be shared with unaffiliated parties. This means you're letting our client collect information such as which apps are on your phone, how and when you use them, data about your activities and content within those apps, as well as how other people interact with you or your content within those apps. You are also letting our client collect information about your internet browsing activity (including the websites you visit and data that is exchanged between your device and those websites) and your use of other online services. There are some instances when our client will collect this information even where the app uses encryption, or from within secure browser sessions. Tap "Submit" to apply for the project; should you be eligible to participate, you will be instructed on how to download the research application. During the installation process, you will be provided additional information regarding the project and our client and required to accept all project disclosures prior to completing the installation. By installing the research application, you're also agreeing to keep this*

> *research, and your participation in it, strictly confidential, and to not disclose any information about this project to third parties. We appreciate your participation. You can stop participating in the research at any time by simply uninstalling the research application. Please contact Applause at applause-research-team@applause.com for greater assistance and detailed uninstall instructions.*

Second:

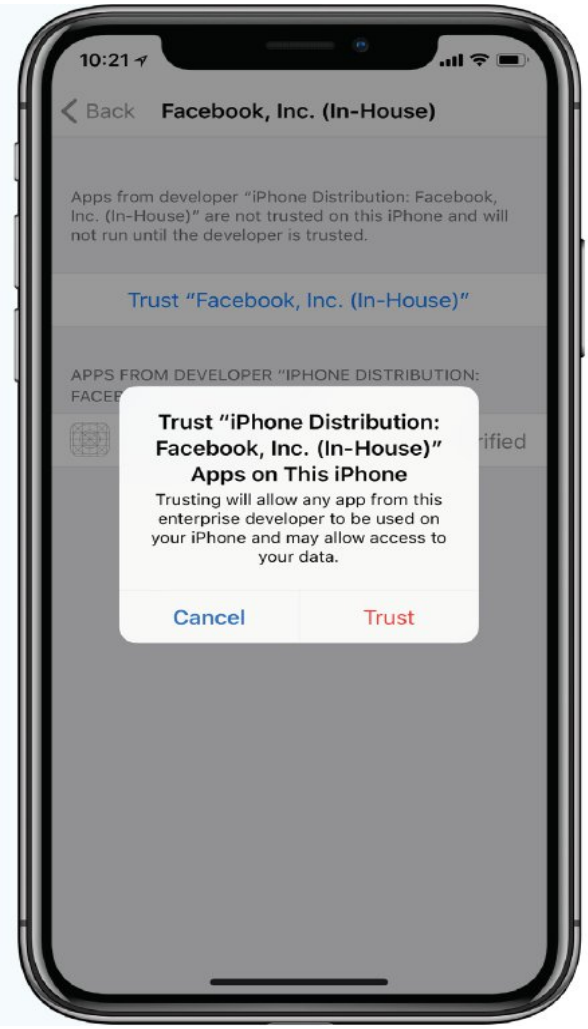
> *Thank you for participating in Facebook's research about how people use apps. This research helps Facebook understand how people use mobile apps so we can improve our services and introduce new features for millions of people around the world. In order to do this, we ask that you install our research software on your phone. Here, we'll explain a bit how we collect information from this software and what it means for you.*
> *By installing this software, you're giving us (Facebook) permission to collect data from your phone that will help us understand how you browse the internet, and how you use the features in the apps on your device. This data will only be used by Facebook, and won't be shared with unaffiliated third parties.*
> *This means you're letting us collect information such as which apps are on your phone, how and when you use them, data about your activities and content within those apps, as well as how other people interact with you or your content within those apps. You are also letting us collect information about your internet browsing activity (including the websites you visit and data that is exchanged between your device and those websites) and your use of other online services. There are some instances when we will collect this in formation even where the app uses encryption, or from secure browser sessions.*
> *Please enter your Username and Password below to agree to participate in the research. By doing so, you're also agreeing to keep this research, and your participation in it, strictly confidential, and not disclose any information about this project to third parties.*
> *We appreciate your participation. To do so, please contact Betabound at [atlas@betabound.com] for uninstall instructions.*

Downloading the App
After registering and agreeing to the survey, potential participants received a link to download the App. The App was clearly branded as a Facebook app as shown in this screenshot of the iOS experience:

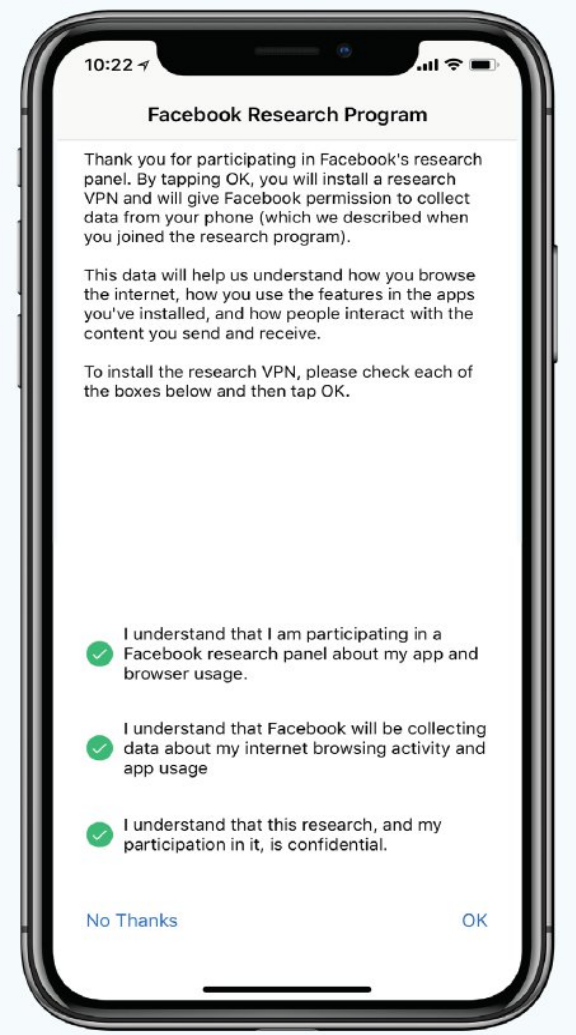


Beginning Installation

During the installation process, the App consent flow provided by Facebook and the iOS installation screens together notified participants repeatedly about the nature and purpose of the app. Once they had downloaded the App, participants were required to begin the installation process. To do so, an iOS screen in this flow gave them the choice of whether to "Trust 'iPhone Distribution: Facebook, Inc. (In-House Apps)" and explained that "[t]rusting will allow any app from this enterprise developer to be used on your iPhone and may allow access to your data":



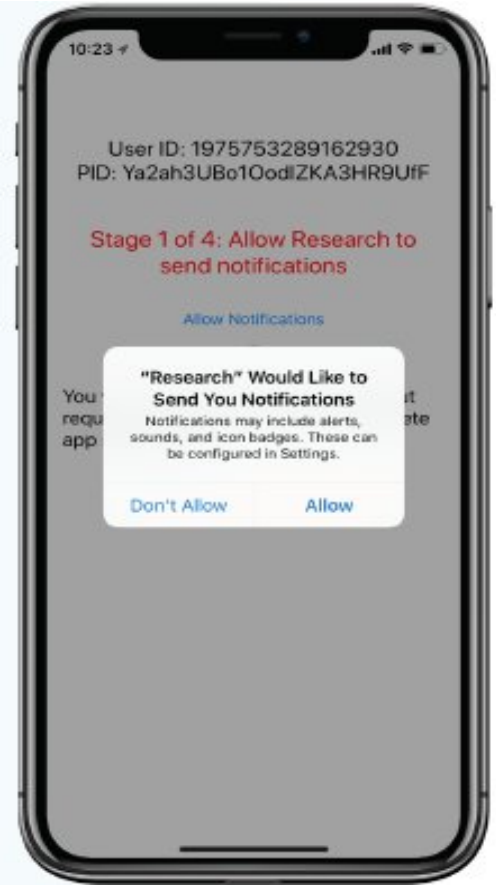
Once they had begun the installation process, participants were presented with a screen explaining that "[b]y tapping OK, you will install a research VPN and will give Facebook permission to collect data from your phone. . .. This data will help us understand how you browse the internet, how you use the features in the apps you've installed, and how people interact with the content you send and receive." Underneath this statement, users were then required to affirm that they understood that they were "participating in a Facebook research panel about my internet browsing activity and app usage."

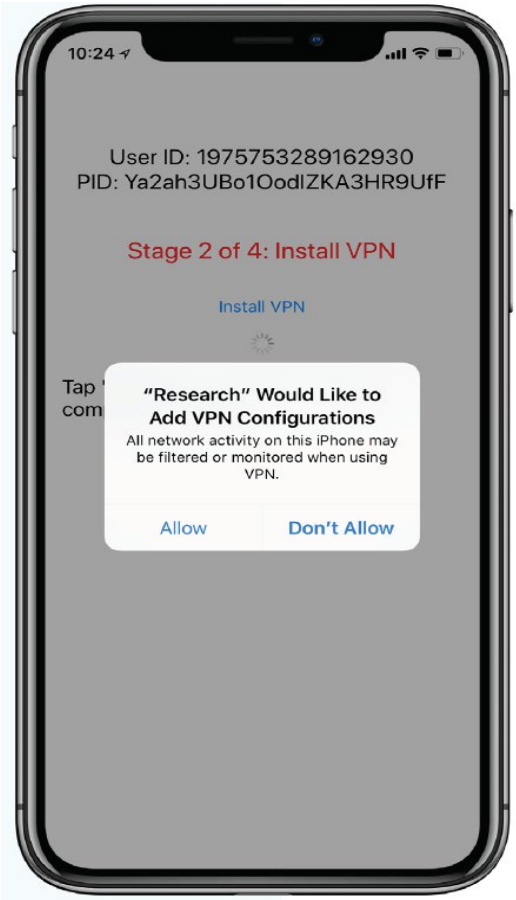


Notifications and VPN Permissions

Next, in this flow the iOS screen requested permission for the App to send the participant notifications and to add VPN configurations. The screen requesting permission to add VPN configurations stated: “All network activity on this iPhone may be filtered or monitored when using the VPN.

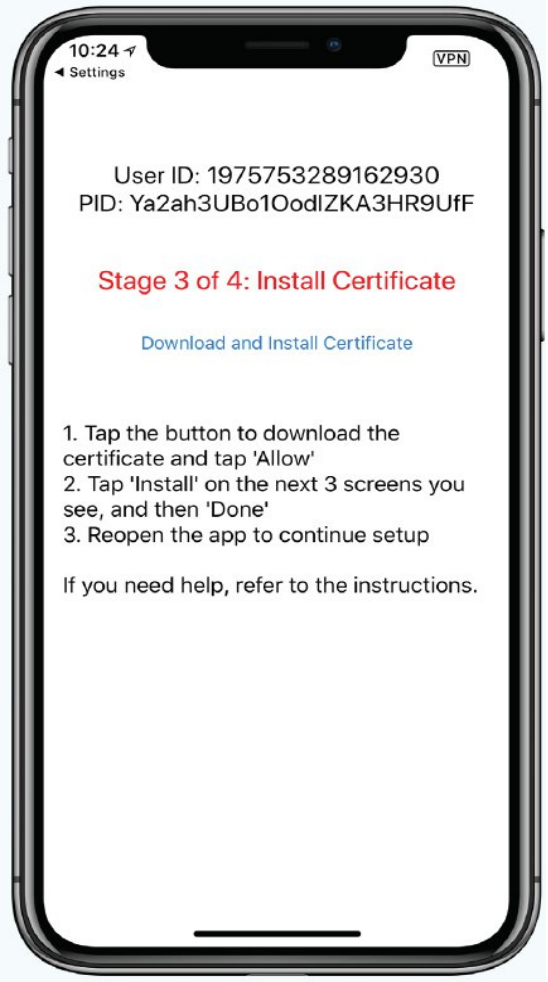
Address: 1601 Willow Road
Menlo Park, CA 94025

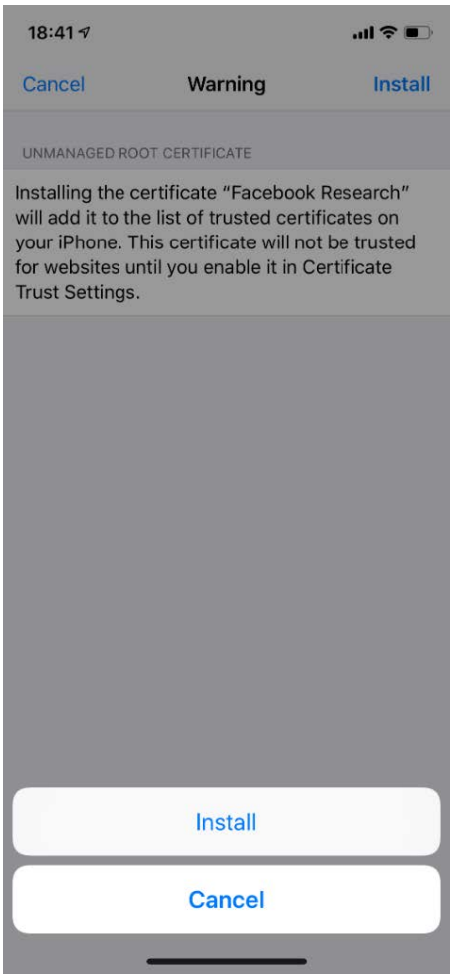




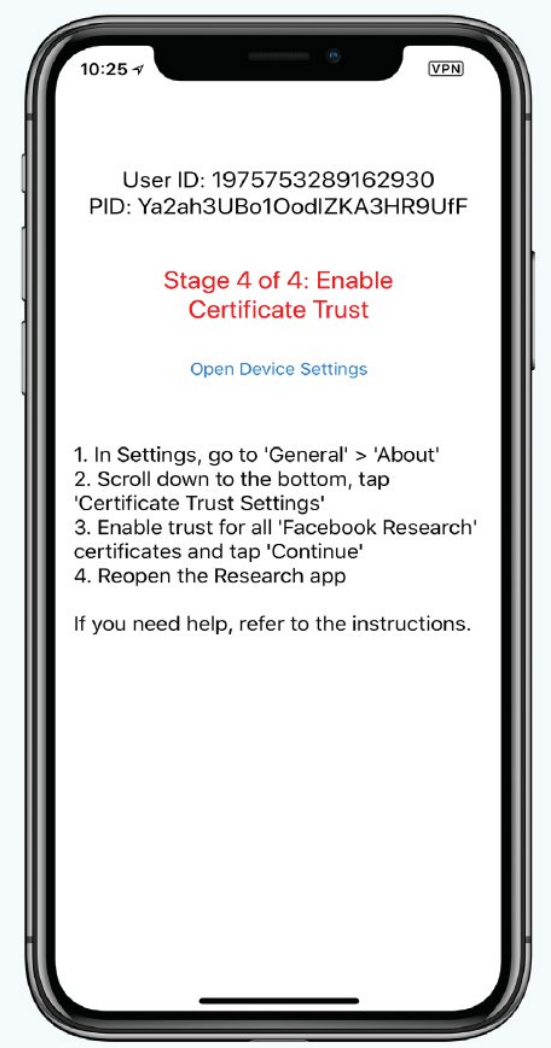
Certificate Permissions

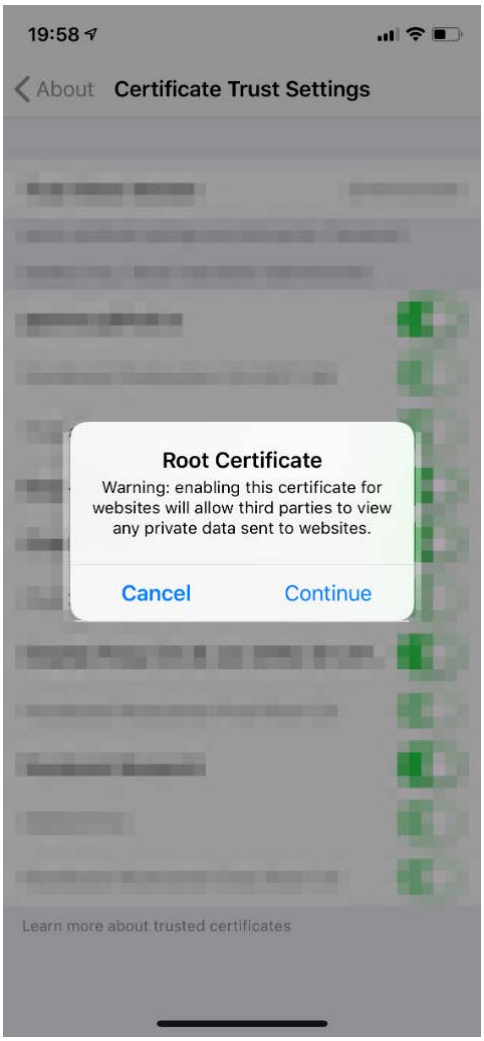
Next, an App screen in this flow requested that participants "Download and Install Certificate" to continue with the App's installation. Before the certificate was installed, an iOS screen informed the participant that it was an "unmanaged root certificate," and that "Installing the certificate 'Facebook Research' will add it to the list of trusted certificates on your phone."





In this flow, the App next requested that participants "Enable Certificate Trust." To do so, participants were required to press "continue" after receiving an iOS screen stating: "Root Certificate [-] Warning: enabling this certificate for websites will allow third parties to view any private data sent to websites."





Once users had done that, their phone settings stated that the application's profile contained such a certificate. (Please note that the Android flows are similar, with variations due, in part, to operating system steps.) Notably, users were also informed that they could withdraw from the research and uninstall the app at any time.

With these facts in mind, below are responses to your specific questions.

1. Do you think any user reasonably understood that they were giving Facebook root device access through the enterprise certificate? What specific steps did you take to ensure that users were properly informed of this access?

As described above, all panel participants received robust disclosures in plain English about the nature and purpose of the App before installing it. Accordingly, participants reasonably understood that they were providing Facebook with access to their data, irrespective of the precise technical means used to do so. Apart from

Address: 1601 Willow Road
Menlo Park, CA 94025

the onboarding disclosures, Facebook made additional disclosures during App installation that connected the technical steps to the nature and purpose of the App.

As a technical matter, the Facebook Research App did not have "root device access" on any device. Rather, the enterprise certificate was the technical means to allow participants to install an app on their phones directly from the internet instead of Apple's App Store. In addition, participants installed a root CA certificate, which is the technical means that enabled participants to share their data usage. In the flow above, the App was clearly listed as an "Enterprise App," and participants had to affirmatively consent to trust the App after being notified that "[t]rusting will allow any app from this enterprise developer to be used on your iPhone and may allow access to your data." Participants were also informed that they had to affirmatively "Enable Certificate Trust" and could only do so after receiving an iOS screen stating: "Root Certificate [-] Warning: enabling this certificate for websites will allow third parties to view any private data sent to websites." These disclosures matched the disclosed purpose of the App to conduct market research from participants who chose to opt-in to the panel in exchange for payment.

2. Do you think any user reasonably understood that Facebook was using this data for commercial purposes, including to track competitors?

As described above, during the registration process, potential participants were informed that the research would be used to help "understand how people use mobile apps," "improve . . . services," and "introduce new features for millions of people around the world." And during the installation process, participants were notified that data collected would help Facebook "understand how you browse the internet, how you use the features in the apps you've installed, and how people interact with the content you send and receive." Participants were also required to affirm that they understood that they were "participating in a Facebook research panel about my internet browsing activity and app usage." Participants were paid by the vendors in exchange for their participation in the research panels.

3. Will you release all participants from the confidentiality agreements Facebook made them sign?

We are happy for anyone who participated to talk about their experiences, and we've told this to our research partners.

4. As you know, I have begun working on legislation that would require large platforms such as Facebook to provide users, on a continual basis, with an estimate of the overall value of their data to the service provider. In this instance, Facebook seems to have developed valuations for at least some uses of the data that was collected (such as market research). This further emphasizes the need for users to understand fully what data is collected by Facebook, the

full range of ways in which it is used, and how much it is worth to the company. Will you commit to supporting this legislation and exploring methods for valuing user data holistically?

We've appreciated our constructive engagement with your staff regarding your legislative proposals to protect people's privacy. We are strongly supportive of efforts to increase transparency around people's information and look forward to further collaborating with your staff on these proposals.

We believe that it's important for people to understand what data organizations collect about them and how it's used. It should be made clear, however, that participants in market research are often compensated as incentives that reflect the time and resources required for them to participate. In the case of this research project, that compensation may reflect things like the time required to set up the app, any additional fees accrued on a participant's network data plan, and time for additional survey follow up.

5. Will you commit to supporting legislation requiring individualized, informed consent in all instances of behavioral and market research conducted by large platforms on users?

Although we believe, as illustrated above, that the information we provided participants and the consent flows in this case were very clear, we are happy to have a conversation about appropriate safeguards surrounding market research. As you know, we are not generally opposed to regulation; Facebook is absolutely committed to working with regulators and legislators to craft the right regulations and legislative framework.

Thank you again for your questions. I look forward to a continued dialogue with you on these important issues.

Sincerely,

Kevin Martin
Vice President, U.S. Public Policy

Address: 1601 Willow Road
Menlo Park, CA 94025